299779

October 8, 2004

Federal Motor Carrier Safety Administration
U.S. Department of Transportation
400 Seventh Street, S.W.
Washington, D.C. 20590-0001

Comments Re : FMCSA-2004-18940 - 44
Electronic On-Board Recorders for Hours-of-Service Compliance

Dear Mr. Hoemann:

The comments herein should serve as thought for developing the next generation of HOS record-keeping that should coincide with the benefits of mobile realtime communications and in-vehicle performance monitoring systems. With proper regulation and timely implementation, communication methods and devices that today serve only niche markets at a premium can be cost-effectively utilized in all forms of new vehicles produced tomorrow. Solutions as to the physical designs of onboard recorders are not discussed, however the theoretical applications and effectiveness are expressed for public, commercial, and government evaluation.

Responding first to the questions in "Issue O" should give a cursory inspection of where I believe government regulation can do the most benefit. The numbered comments correspond as follows:
(1) FMCSA should require compliant carriers to use EOBRs that are only factory-installed.
(3) The minimum information automatically recorded by EOBRs should exceed NHTSA's minimum requirements for Electronic Data Recorders (EDRs) in automobiles.
(4) Drivers should be required to enter their identities via a bioprint scanner and status via a touchscreen.
(5) FMCSA should require all factory-installed EOBRs to have Differential GPS for maximum precision.
(6) Fingerprint scanners should be of an industry standard with an adaptation means to include a facial bioprint scanner to verify the identity of a driver in CMVs having multiple drivers whenever the EOBR is recording the vehicle as driving-time.
(7) The EOBR should cross reference a bioprint from an onboard realtime device to validate the driver's identity for sharing Duty status with a smart memory card.
(8) Open-source transfer protocols for factory-installed EOBRs should be required as a federal standard.
(9) Factory-installed eyelid scanners along with an EOBR should allow for more driving-time.

Comments on Issue A : *Synchronization of Recorder to a Vehicle Operation Parameter*

Vehicle manufacturers have already implemented solutions to identify their vehicles' performance relative to real world conditions. Vehicles in themselves have become computers with wheels that collect information from monitoring (sensing) devices integral for efficient mechanical operation within its engineered parameters. The FMCSA should require all U.S. truck makers to include monitoring systems common to the vehicle's internal databus be recordable by the EOBR in realtime, as well as transmittable to the home-base, for documenting the safe operation within regulatory parameters.

Comments on Issue B : *Amendment of Records*

I believe any EOBR system or method that allows true data to be altered will encourage falsifications with the same motives as to why some drivers carry multiple log books or manipulate status entries. The driver however should be able to select a predetermined Remark from a menu listed on a dashboard viewscreen and have it added to the EOBR as a late entry associated to a time prior. Default conditions for on-duty-not-driving should ensure proper status relative to the CMV's motion so that Remarks or actions to amend Duty status are not available or permissible.

The key objective for utilizing electronic data recorders should be for the true documentation of history. EOBRs should collect data from points within the vehicle and record it in sequential time to memory. Like automotive EDRs, commercial EOBRs should not have the ability to erase or change any single desired point of data from its memory. Again in similarity to EDRs, the only erasure to occur should be when the memory capacity is full and the earliest data is completely deleted to allow for current data to be added. But unlike EDRs that record over a several second loop, EOBRs should have a larger memory capacity for a several day loop.

Comments on Issue C : *Duty Status Categories When the CMV Is Not Moving*

The problem of accurately documenting history becomes muddled when data entry is dependent upon human actions - for example, the phrase "I forgot to clock-out for lunch". Factory-installed EOBRs should be integral to the keyswitch and vica versa to alleviate these types of human errors that effect Duty status through default settings, whether unintentional or deliberate, when the vehicle is parked.

Keyswitch designs should be required such that the engine may be turned-off but the key cannot be removed unless the driver identifies the status on a touchscreen menu. Drivers who choose to shut-off or idle the engine with the parking brakes applied are automatically entered upon location for on-duty-not-driving status unless changed via the touchscreen. This requirement for all new trucks should allow for local carriers to opt-out through a wireless telematics service provider (TSP) or at the dealership.

The truck itself must be able to distinguish legitimate places for changes in status while not in motion. Since time and space are relative, EOBRs integrated with Graphic Information System (GIS) technology will prevent such action of declaring not-driving status while stuck idling/parked in traffic. Therefore, the benefits of factory-installed Differential GPS (DGPS) should further provide the correct time to legally change status based upon true location.

Sensors currently deployed in automobiles to detect seat occupancy and door/trunk-lid status should also be included as EOBR inputs in CMVs to assess default assumptions by the embedded HOS software program while idling. The program should automatically default to on-duty-not-driving status whenever the CMV is left idling in a GIS authorized location and then the driver's door is opened and the seat unoccupied. Automatic status changes while on a roadway may occur when vehicle collision/ engine malfunction inputs are included in the program. There should be no automatic status change to sleeper-berth since drivers know they will be cheating themselves of driving-time if they forget to manually change status - for the contrary, eyelid scanners would document false sleeper-berth status claimed while on-duty. Drivers that turn-off the engine but fail to remove the key or manually enter a status change should default the status automatically to on-duty-not-driving when the driver's door is opened and then the seat is vacated. Automatic status change to on-duty-driving should occur when the brakes are released, unless first manually entered as off-duty.

It should be understood that requiring carriers to use retrofitted EOBRs for automatic duty status information would be too cost prohibited to include GIS/GPS systems, bioprint systems, safety systems, etc., for implementation of automatic duty status entry. Paper RODS should continue to be utilized for legitimate and illegitimate recording until such a time where the national fleet of trucks all contain factory-installed EOBRs with automatic HOS monitoring that have the same operating standard requirements.

Comments on Issue D : *Ensuring That Drivers Are Properly Identified*

The FMCSA should require biometric ID of drivers, especially in this age of terrorism. Factory-installed EOBRs integrated with a dashboard mounted fingerprint scanner should allow for any bioprint to satisfy authorized access to the Duty status menu and vehicle operation by default - that is, the unit doesn't discriminate unless programmed for a specific bioprint(s). Motor carriers may then choose to set identity recognition from the company's identification database with its own driver's biometric algorithms at the home-base through wireless telematics in realtime. In addition to the EOBR recording the driver's

algorithm, the vehicle owners that utilize TSPs would know the driver at any given time and may sanction a defensive response for non-identification - for example, disabling the engine throttle. EOBRs containing digital biometric identification downloaded via a TSP would also serve as an anti-theft device - example, not allowing the engine to start or even crank. Carriers and owner-operators that choose not to have wireless support services but desire the anti-theft feature of EOBRs would need to have a bioprint entered at the dealership as the proprietary administrator's password to enable/disable appropriate factory settings via the touchscreen.

Ensuring that drivers are properly identified should encompass all licensed drivers. The mere photographing of licensees does not go far enough to ensure validity. The practice of forging documents to obtain legitimacy is prevalent in this age of high tech scanners, digital manipulation and printers. In addition, State DMV examiners have been arrested for violating the public's trust by issuing fraudulent licenses. There must be a means to ensure validation by the issuer of the document, namely the collection of a digital fingerprint at the DMV that is instantly compared and entered in a national database.

A National Identification Verification System should benefit motor carriers as a means to quickly validate a driver's true identity by electronically transmitting a realtime bioprint from a keyboard (just recently marketed for PCs) along with a name or Social Security Number. A true or false response is all that is needed in return from the repository. Moreover, company persons authorized to access data from a National Driver Record Identification verification database maintained by State DMVs can validate the driver's license status.

As a U.S. citizen, I have no objections to have my name, face, Social Security Number, driver's license or digital fingerprint in a federal repository when it ensures the certification of my identity. It would verify that my bioprint is the only valid password for my authorized access that cannot be lost, forgotten, stolen (sic), duplicated or otherwise compromised for a myriad of applications. Further comments as to the merits and public use of a national "true/false" identity database is not an issue at this time.

Comments on Issue F : *Audit Trail*

Motor carriers that utilize the service of TSPs for day-to-day operations and internal reviews can document the driver's HOS, which should be sufficient for compliance review at the place of business. Factory-installed EOBRs can and will only record the vehicle's HOS and the driver(s) ID, which should be sufficient for roadside audits if the EOBR lists only one dedicated driver. With the requirement that all CDLs issued from all states contain a "smart-chip", the driver's license itself can become an event log of vehicles used and times driven such that an official on the highway can confirm driver HOS compliance on location if/when the EOBR indicates multiple drivers in its memory.

"Smart CDLs" should be the standard method required to verify driving-time by motor carriers whose drivers share vehicles or drivers without the realtime wireless services of a central station database. Today the retail, banking and medical industries are distributing large memory SmartCards at a cost of $15 according to *Newsday*, September 19, 2004. By the time Motor Vehicle Administrators agree upon a unified method of identification using biometrics, the cost of adding a smart-chip to all new CDLs and renewals will be insignificant - less than $2 per year charged to the licensee to cover DMV equipment and software implementation. Embedded smart-chips everywhere should provide economies-of-scale in the not-too-distant future such that operational cost would not be the true barrier for Smart CDL implementation by State DMVs.

There should be no recording device used for compliance that allows data to be changed once captured. In addition, the microprocessors used within devices must recognize and document input errors. It's the computer's software that must be able to distinguish whether the error is either a sensor malfunction or input tampering and to record/signal an alert response.

The FMCSA must require all software used in EOBRs and back-office mainframe computers use open-

source protocols and display in a single standard format such that audit teams may verify that a carrier's historic records are unable to be changed at a later time by someone's keyboard through a program's secret backdoor access. It should also stop clandestine activity and hackers (internal and external of a motor carrier, TSP, or software vendor) from corrupting true data stored. Open-source programming of EOBRs, in addition to preventing covert modifications, should further detect and record sensor tampering since it should also be comparing time and distance data recorded from the GIS/GPS system.

Roadside auditors should be able to quickly review compliance through the vehicle's dashboard viewscreen. Direct data extraction from the EOBR should be reserved for accident investigations or for auditors to use in the event of a malfunctioning dashboard display.

Comments on Issue H : *Verification of Proper Operation*

The electronic chip makers have made such design advances for extreme environments that today NASA still has two mobile vehicles on Mars that are performing past their intended timetable. Solving such issues have made the advancements and practicality of using electronics for Earth vehicles quite reliable. RPM sensors used for ECM ignition and fuel injectors rarely fail on the road (How many people still drive carbureted cars today?). 100,000 mile tune-ups are common and the last fuel pump I had to replace was on a 150,000 mile car. But with trucks there should be some verifiable means of compliance due to the probability of having a vital EOBR sensor or other required input module fail in the lifetime of a 500,000+ mile vehicle. However consequent, the sensors that also provide vital information for safe operation of the CMV usually warrants a tow service upon communication malfunction anyway.

EOBRs should contain read-only memory that performs and documents a self-check of its inputs as well as constant monitoring of their performance to within each specification. Included in its self-check should document the results of self-tests of modules that control the other systems integral for HOS. The truck's ECM, for example, has a self-test upon start-up that should include sending a signal through the vehicle databus to the EOBR of a code that indicates "OK" or identifies a specific data component that has failed HOS compliance. The EOBR should also record the results of self-tests of the GPS receiver, biometric scanners and card readers, the telematic control unit (TCU), etc. and plainly indicate the component(s) failure (not just the code numbers) on the dashboard viewscreen along with its level of concern.

Levels of concern are a matter of priority for each component function in documenting HOS that can or cannot be substituted for a defined period. For example, signal loss of the odometer to the ECM databus may allow days for repair since the GIS/GPS is also providing time and distances traveled. The loss of the GPS while the odometer is broken should indicate and warn the driver that a repair is needed within hours. EOBR failure should indicate RODS are immediately required for a limited time until replacement.

Calibration of EOBRs should be unnecessary due to its high quality design requirements. There should be no serviceable or adjustable components within electronic modules. Sensors that are out-of-spec should be replaced without the option of repair tampering.

Comments on Issue J : *EOBR Maintenance and Repair*

In accordance with the previous opinions above, an EOBR should have the same required maintenance and calibration as an automotive EDR - i.e. none. With perhaps the exception of the GPS receiver, none of the other data devices used for HOS compliance should be repairable. Wire harnesses used for the sharing of data on the vehicle's communication network should be the most labor intensive to replace if not repairable.

The only malfunction that should cause the EOBR to fail its self-check would be its inability to record. The cause of which should be from an embedded chip. Funds should be allocated to develop EOBRs that have chip redundancy including excess memory for in-service longevity in case some chips fail.

Memory storage methods utilizing a mechanical means should be prohibited since trucks inherently vibrate and are susceptible to all sorts of environmental conditions.

EOBRs that fail should be replaced, tagged by a mechanic or technician and kept for a defined period by the carrier. EOBRs should be of such an operational standard and configuration that any make truck can accept any FMCSA certified manufacturer's tested EOBR, be it from another truck maker or an aftermarket equipment vendor.

Data extraction from a failed EOBR should only be performed from a FMCSA certified technician. The extracted data should be copied in a pdf format and accompanied with a paper copy. Documentation as to the historic data should include the technician's certification number, the date, the EOBR's internal serial number (it should match the nameplate serial number), nameplate certification number, and the technician's signature.

Comments on Issue K : *Development of "Basic" EOBRs To Promote Increase Carrier Acceptance*

Basic aftermarket EOBRs should include GIS/GPS technology, a touchscreen display, a USB access-port for a laptop/printer/tablet PC, and a telematic control unit (TCU) having a receptacle to plug-in a TSP wireless modem. Hardwire installation in a CMV for recording engine status should be available only to CMVs with ECM technology. Earlier model trucks should be allowed to die without mandating a costly retrofit model requiring extensive labor, hardware, wiring, and electronic sensors for 3 reasons; (1) large long-haul carriers don't have many 15 year-old trucks in their fleet; (2) small carriers or independent owner-operators aren't going to invest thousands of dollars for an electronic recorder in a high-mileage vehicle especially when RODS have sufficed; (3) older model CMVs that aren't junked are sold to log-book exempt companies.

Carriers though may be interested in retrofitting the remaining fleet that does not have factory-installed EOBRs if the cost of updating can provide asset management and travel efficiencies. In order for the FMCSA to benefit from electronic HOS records, there has to be a business return on investment that additionally provides a greater benefit to the company by the use of its shared realtime data inputs.

A basic factory-installed EOBR should be required of manufacturers to ensure that all CMVs are electronically HOS compliant in 15-20 years through the turnover of replacing a national fleet. Local carriers that purchase new trucks can and should utilize the datalinked systems of the EOBR for the value-added safety, security, management and travel efficiencies.

Original equipment and systems that address safety issues should also share data with the EOBR that can be utilized for automatic HOS in which driver fatigue can be measured. Aside from plugging-in an umbilical cord from the EOBR to the driver, an alternative method currently in development consists of a camera that monitors the drivers eyelids. If the system can operate at night, software detection of the eyes-closed for more than 2 seconds should trigger an audible alarm within the cab and record it to the EOBR memory. Two alarms within 5 minutes should then disable the throttle and the alarm to continue until the truck stops. This type of requirement may yield to HOS rule changes that allow for more driving-time in the future, especially when Intelligent Highway infrastructure and telematics are applied.

Factory-installed EOBRs should also take note of lane accuracy that may signify either driver fatigue or mechanical difficulties. Both are unsafe to the traffic community. Lane Departure Warning systems will also correct bad driving habits of some drivers that do not signal their intentions (the drivers that do signal all the time won't even know their CMV even has this safety system). So why should the best drivers have to pay for this? They don't if its a company vehicle, if they're owner-operators then its the price for early adaptation to a national standard. More importantly, motor carriers should benefit in the assurance that their drivers' actions aren't a liability to their insurance rates.

Factory-installed EOBRs should be required to capture the driver's biometric identity. The use of

fingerprint algorithms for viewscreen access to the HOS menu in changing status should be the adopted standard. However, EOBRs should be adaptable to accept an alternative method of biometric identification for carriers that employ team drivers. An aftermarket facial bioprint scanner that captures the driver's algorithm a few times per hour can confirm that the drivers haven't switched - i.e. unless the team consists of identical twins. This method would also have to be certified for night-driving recognition.

All factory-installed EOBRs, regardless of the truck make or model, should be required to display the archived data as well as the HOS menu on the dashboard touchscreen in the same format. Viewscreens should also be of a standard frame and pixels. Roadside audits, if not viewable from the dashboard display, should also be in the same format suitable for a tablet-like PC for official/company access via a single standard connection.

Factory-installed EOBRs of course should integrate GIS/GPS technology for documenting locations and confirming the accuracy of the CMV's onboard clock. GIS/GPS can also document the amount of time spent not-driving while at a shipper's/receiver's location. The benefits of GIS/GPS technology in improving the navigational efficiencies for the trucking industry have shown merit towards carrier acceptance.

Factory-installed EOBRs should include some data ports that can be used by carriers with team or slip seat drivers. Specifically, the data supplied would be used for a memory card device to record an individual's HOS for required carriers. The EOBR data input ports should be dedicated for facial bioprints and smart card identification. Owner-operators should be able to utilize the "audit-port" for compliance in retaining a 6-month archive.

It would be advantageous to require EOBRs to be of modular datalink design such that its internal components serve to collect, record and read information only. As a result, an EOBR failure would not effect the collection of HOS data by the home office using a TSP or viewscreen control for the driver. It would also provide the carrier a means to verify EOBR recordings. Conversely, EOBR recordings should also validate the carrier's compliance database. Most importantly, a basic standard read/write EOBR would be inexpensive to replace than models that contain GPS receivers, realtime communication systems, dispatch and vehicle performance softwares.

It should be required that the information systems necessary for automatic HOS status be equally available to the carrier's home-base, or a home PC as the case for the OTR owner-operator, in realtime through low-cost TSP modems of customer choice. This is a huge barrier that prevents motor carriers with a mixed model fleet to cost-effectively manage their assets in realtime. Furthermore, proprietary TSPs affiliated with the manufacturer do not return data to the vehicle that the driver can use in realtime to foresee traffic status or receive hazard and construction warnings. Navistar International charges their customers TSP services for home-base monitoring but mainly collects the ECM and vehicle performance data for product evaluation.

Comments on Issue M: *Potential Benefits and Costs*

To put this in a realistic business perspective, its aspects should be viewed from the bottom-line as cost versus the financial benefits. Given the estimate that a $500 factory-installed EOBR is equivalent to a $3000 retrofit EOBR, a $3000 factory-installed EOBR should include integrated systems that make automatic HOS for compliance possible, asset management for even the smallest of carriers practical, and improved safety systems for the drivers within the traffic community. Add the profit margin for the truck makers and the price should be about $7000 to the truck buyer. If the truck is intended to be used by the original owner for 10 years in a fleet, can the value-added data systems be used to prevent $700 in lost time, wasted fuel and down-time per year? Absolutely.

The operational benefits described in the last paragraph concerning EOBR integration with other logistics management systems will not improve productivity. Current realtime communication systems used by

carriers only improve efficiencies for logistical management and do it without EOBRs. Productivity is always the result of the worker, in this case it's the drivers whose company productivity depends upon moving as much freight from one point to another in the least amount of time. Unless EOBR requirements provide realtime data exchange that is beneficial to the driver, the efficient use of time to make money will continually be lost to an unwitting driver's decision in choosing the wrong way to go - be it not finding a delivery point right away to using a highway that has a 2-hour backup. Giving drivers the ability to foresee a destined location on a status-map display in advance of arrival ensures that a driver will keep moving without making poor route choices with unforeseen consequences.

Some providers of telematics services are beginning to include traffic reporting as well as the navigational benefits of GPS. The inability for TSPs to have equal access to vehicles prevents a competitive market in which the CMV owner truly benefits. Case in point, new CMV purchasers would be required to pay several thousand dollars for an EOBR and supporting systems as standard equipment that may not be compatible with the wireless method of its current TSP. Does the buyer have to specify the TCU for proprietary wireless data exchange? Does the next owner of the CMV have to trash the TCU and replace it with a TCU that is compatible for a different TSP that he/she wants?

All new vehicles should contain TCUs as the only wireless interface with a vehicle's databus. In this manner, the information derived from system modules and sharing the same databus can be graphically and textually depicted on the dashboard viewscreen while maintaining back-office compliance/services. Current business models offered from vendors are to add a telematics recorder with multiple functions to each CMV at a sizable cost that is reflected in a monthly payment per vehicle for a leased term.

More should be required, perhaps with help from the FTC, such that telematics services into GPS embedded vehicles is an open market to compete for customers without the high cost of equipment retrofitting of fleets. That is to say that if a TSP could access any CMV with a $15 modem instead of installing a $200+ TCU per vehicle, more TSPs could enter the market with superior back-office services that are beneficial not only to the fleetowner but moreover in providing realtime travel services to the driver. More independent TSPs with equal access to vehicles means better services at the lowest cost to motor and coach carriers.

It is unknown what the true cost of a fully automatic factory-equipped EOBR CMV would cost at this time. However, the cost of an EOBR that is required to be an independent module and serves only to read and record memory from ECM, GPS and relative monitoring systems or devices would be quite inexpensive to replace upon failure because its data output would not be vital for the datalink operation of the other in-vehicle system modules or sensors common for wireless and vehicle databus exchanges.

With the economies-of-scale theory applied, the first model year that requires EOBRs and associated support systems will cost the manufacturers more to produce than the one millionth one installed. Under those rules, the first year purchasers of factory-installed EOBRs unfortunately pay more for automatic HOS (whether they need it or not) than those who buy CMVs in later years.

Comments on Issue N : *Incentives To Promote EOBR Use*

The eventual requirement that all new CMVs contain EOBRs for public safety benefit should make for a transparent playing field for many competitive markets in which law compliant players are no longer at a disadvantage to those who cut corners. With equipment cost aside, opposition to EOBR documentation of compliance should be from those that don't want the truth to be seen. Eventually they will have to own a factory-installed EOBR in which compliance is transparent, or find another line of work to cut corners. Fortunately, the young and newly licensed professional drivers of the future should find automated HOS favorably and acceptable because they were (are) raised in a computerized society at an early age.

Incentives for new CMV purchase should be for owners to exploit the in-vehicle support systems of an EOBR that also makes efficient use of time without costly mistakes for the lifetime of the vehicle owned.

The aforementioned eyelid monitoring system, from a Tier 1 supplier such as Delphi for example, should allow for a true 12-14 hour highway driving-time regardless of the not-driving hours logged for a day. GIS/GPS navigation has proven to lessen the likelihood of losing time. Competitive TSP access to vehicles should bring lower service cost for asset management to benefit carriers and aid in realworld navigation for the driver's benefit in realtime. And embedded safety systems that avoids collisions...well, we all should know how expensive and heartbreaking that experience can be.

Supplemental Comments :

Further discussion is necessary related to comments of biometric devices. The success of bioprint identification as a means for allowable access will be entirely dependent upon a data server's ability to verify that an input algorithm is actually received from a realtime scanner. Extensive research and development of open software must be specifically employed for identification data servers so that authentic algorithms derived from a memory source are identified and rejected.

The aforementioned introduction of a newly marketed keyboard with an embedded fingerprint scanner raises concerns about a Microsoft product. If it works as a realtime device in which the algorithm doesn't get captured by the hard drive, it will be a tremendous leap in eliminating many practices of fraud. However, nobody knows for certain what Microsoft software allows to be performed inside our PCs. Despite Microsoft's security patches and claims with each new product that it is the most secure ever, hackers have proven time and again of their ability to find covert access and retrieve information from its customers. If bioprint algorithms are able to be captured and stored in PCs, then hackers will eventually steal and use them for authorized access to accounts and secure networks with the same ease as if entering a stolen alphanumeric password as the means for identification verification.

A benefit described in Issue M : *Potential Benefits and Costs* suggested new trucks contain TCUs that share data with the EOBR and the company's TSP. As such, any and all fleet or individual truck owner can and should have access to the TSP of their choice because of a competitive market of TSPs in which all can and should have equal and low-cost access to any vehicle (cars included). The quality of service at the lowest cost by TSPs would be paramount in retaining customers if the customer could switch modems to a competitor in a manner similar to like replacing a simple fuse.

The requirement that HOS include Place Names and State Boarding Crossings pose an increased cost for EOBR memory and software processing of the GPS data. GIS systems should contain the software module and read-only memory of PNs and SBCs so that the GPS data will trigger the associated code to be recorded by the EOBR through the vehicle's high-speed data network. In this manner, the likelihood of EOBR processing failure is lessened with the added redundancy that recorded raw GPS data, also supplied through the common databus, can be used alone to note locations from the back-office or "audit-port" software applications. In addition, any required update/replacement may be performed by changing the PN/SBC module in the GIS instead of an entire EOBR replacement.

The required automated data captured by an EOBR should reflect only Duty status and vehicle event data for HOS compliance and for accident investigations. Other than bioprints and manual changes to status, I fail to see the need to waste storage capacity in an EOBR on preloaded data that doesn't reflect the driver's/vehicle's performance. The objective of a fully automated and accurate factory-installed EOBR can be compromised with each data entry from a human source. Therefore, review of shipping documents and cargo should still remain as paper in the possession of the driver until such a time when bills-of-lading become paperless. Even at that, it should still be stored somewhere else.

Wireless phone carriers should be consulted as to the merits of high-speed 2-way data service capabilities of 3rd generation systems for HOS carrier compliance. Nonprofit engineering organizations should validate the technical specifications and performance requirements of vehicle systems and components. Academia, as well as government agencies and public-interest groups, should contribute certification of open protocols.

Of all the comments expressed, the suggestion of eyelid scanners as a required input for factory-installed EOBRs should be studied most closely. If it can be perfected to perform with minimum (lens cleaning) maintenance and be tamperproof, true fatigue can be monitored and exposed to those without common sense. As a result, drivers should be credited with sleeper-berth status anytime that is advantageous to them. Furthermore, false claims manually entered as off-duty/sleeper status would be suspected when the EOBR documents eyelid scanner alarms within hours of returning to driving-time. Lastly, employers/shippers that push the drivers to the point of triggering fatigue-alarms should be fined beyond common cents.

The requirements for data access by road officials should be specifically defined as to not encourage a political jurisdiction to exploit EOBRs as a revenue source. The conditions for direct access to EOBRs was discussed in Issue F : *Audit Trail* , Issue J : *EOBR Maintenance and Repair*, and Issue K : *Development of Basic EOBRs To Promote Increased Carrier Acceptance*. It should be obvious that reviewing un-signaled lane changes, for example, can empower law enforcement to issue tickets for moving traffic violations in which the officer did not witness in realtime. Officers that prefer to slack-off in their duties of traffic patrol will find it much easier to pull over new trucks with EOBRs in order to produce a quantity of summonses satisfactory to his/her administration. The EOBR for its part should be required to record the time and location whenever its "audit-port" is used along with a bioprint of the reviewer. In this manner the carrier should be able to prove in court that the motive for the audit was not for HOS compliance or equipment safety checks but rather for traffic ticketing.

What's more, factory-installed EOBRs should provide crucial information for fatal accident investigators also regardless of the carrier's requirements for HOS compliance. The FMCSA should require EOBRs to record in-vehicle alarm events from yet and upcoming warning systems - i.e. forward-looking radar, tire pressure, air pressure, eyelid scanner, panic braking, etc. With this standard requirement, an EOBR would serve the equivalent of an automotive EDR. The NHTSA initiative should standardize EDRs for automobiles in the same review format as EOBRs. This should make for consistent enforcement practices from a single standard portable device whereupon data access and display of recent history from any vehicle can provide transparencies to investigators across the board. Therefore, every motorist and trucker in the future would be aware that their (proper or improper) performance in operating a motor vehicle will lead to true accountability (0-100%) in the event of a mishap while in the traffic community.

The motor carrier industry as a lobby will not accept EOBRs voluntarily. Carriers that exploit the current method of paper-based HOS compliance as a means to cut corners for increased profits (or to break even) are not willing to lose money for the sake of public safety. Those companies that truly comply know that they are at a competitive disadvantage, and some are probably forced to cut corners now and then. There appears to be a credibility problem within the industry when so many carriers object to a means that eliminates altering records and provides a level playing field.

Indeed, the FMCSA must approach the transition from paper to electronic HOS through manufacturer mandated requirements. Motor carriers that recognize the benefits of automatic HOS will have no privacy problems if it truly is a law compliant business. Those that are not will have to increase their repair budgets to maintain a fleet of older CMVs so that paper HOS can be maintained. Nevertheless, old trucks cannot be perpetually maintained and function efficiently for the long-haul and still remain profitable to operate. When that mandate arrives, there should be no new CMVs offered for sale in the U.S. by any manufacturer without an automated EOBR. As such, new truck buyers no longer will be able to choose one make over another in order to avoid compliance. In time, companies without automatic EOBRs and wireless back-office support will be the ones at a competitive disadvantage.

Sincerely,

B. Reimann